UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/694,824	10/29/2003	Antonio Lain	200205659-2	7594

22879 7590 08/31/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
GERGISO, TECHANE	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/694,824	LAIN ET AL.	
	Examiner	Art Unit	
	Techane J. Gergiso T-G	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06/01/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on June 06, 2007.

2. Claims 1-14 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed June 06, 2007 have been fully considered but they are not persuasive.

4. In response to applicant's arguments, the recitation (Page 6: Last Paragraph: The present invention relates to the distribution of **cryptographic keys which are generated from an ancestral hierarchy**. Such **keys are often used to protect access to subscription services**, for example. The manner in which **the keys are generated means that, once one key is invalidated or compromised, it effectively compromises the security of other keys within the hierarchy at least to the extent that a common ancestry with the invalidated or compromised key is shared**.) has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

5. The applicant also argues that Lotspiech and Sudia are not analogous arts because Lotspiech appears generally relevant to cryptographic keys generated from an ancestral hierarchy and Sudia is related to digital signature. The examiner disagrees with the applicant's argument because the digital signature requires cryptographic key generation, distribution and management and Sudia suggests (0111: the card generates a key pair which is to be used by the user of the card and which the user can have certified as his own by any appropriate desired CA. Then, when submitting a newly generated public key for certification, the device private signature key would be used to countersign the certificate request data, which is already signed by the newly-generated user private key. And [0116] Controlling Access to the Public Key of the Root Certifying Authority and Cost Recovery). Therefore the digital signature can not implements with the cryptographic key and Sudia is analogous art to Lotspiech.

6. Furthermore, the applicant also argues that "the independent claims requires that users are grouped within the key hierarchy. However, in the teachings of Sudia, the key hierarchy is being generated to reflect to the user groups." The examiner disagrees with the applicant's argument, because the applicant did not claim or show the mapping is only from users to key hierarchy. The examiner considered mapping users to key hierarchy is substantially similar to mapping key hierarchy to users.

7. The applicant also argues that "the domains for each group of users within the hierarchy based upon characteristics of access of the groups are not created in Sudia." However the applicant do not explicitly define a domain, and the examiner considered the suggestion in the

disclosure as different types or groups in the hierarchical structure as shown either in figure 4 or disclosed in 0076 as Gold domain, silver domain, and Bronze domain. Sudia discloses such grouping or defining similar organizational structure based X.500 Directory model (0046-0050).

8. Finally the applicant generally alleges the prior argued without specially pointing out the specific features in each independent claims 1, 10 ,13 and 14.

9. For the above given reasons, the applicant's argument is not persuasive to overcome the prior arts in record to place independent claims 1, 10, 13 and 14 in condition for allowance. The applicant's arguments also do not place the dependant claims 2-9 and 11-12 depending directly or indirectly from their corresponding independent claims 1 and 10 respectively in condition for allowance.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-9 and 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech et al. (hereinafter referred to as Lotspiech, US Pat. No.: 7,039,803), in view of Sudia et al. (hereinafter referred to as Sudia, US Pub No.: 2002/0029337).

As per claim 1:

Lotspiech discloses a method of managing security keys generated from an ancestral hierarchy and used to provide selective access to provision of a service, wherein invalidation of a key necessitates reconfiguration of each other key within the hierarchy to the extent another key and an invalidated key share common ancestry, the method comprising the steps of (recitations in the preamble is not given patentable weight):

defining at least two groups of users of the service to whom keys have been issued (column 3: lines 5-21; column 4: lines 37-60; column 6: lines 20-37);

issuing keys to users from domains within the hierarchy upon the basis of their grouping (column 3: lines 11-20, lines 53-64; figure 4:36, 38; Column 7: lines 55-65).

Lotspiech does not explicitly disclose allocating within the hierarchy a distinct domain for each group of users. Sudia, in analogous art, however, teaches allocating within the hierarchy a distinct domain for each group of users (0046-0050). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Lotspiech to include allocating within the hierarchy a distinct domain for each group of users. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a system for securely using digital signatures in a commercial cryptographic system that allows industry-wide security policy and authorization information to be encoded into the signatures and certificates by employing attribute certificates to enforce policy and authorization requirements as suggested by Sudia in (0024).

As per claim 2:

Sudia discloses a method, wherein the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to their perceived value to a provider of the service (0024; 0053; 0055).

As per claim 3:

Lotspiech discloses method, wherein a first user group having the highest perceived value to the provider are allocated keys from a first domain, and wherein keys from the first domain share fewer ancestors with keys from other domains than said keys from other domains share with each other (Column 4: lines 37-50; column 10: lines 3-22).

As per claim 4:

Lotspiech discloses method, wherein keys from the first domain share only one ancestor with said keys from other domains (column 4: lines 40-60).

As per claim 5:

Lotspiech discloses method, wherein the ancestral hierarchy has a binary tree architecture (column 3: lines 15-22).

As per claim 6:

Sudia discloses a method, wherein the at least two groups of users are defined upon the basis of a predetermined policy which provides that users are grouped according to a perceived susceptibility of them ceasing to require the service, and a first user group having the highest perceived susceptibility are allocated keys from a first domain, and wherein keys from the first domain share fewer ancestors with keys from other domains than said keys from other domains share with each other (0024; 0053; 0055; 0046-0050).

As per claim 7:

Lotspiech discloses method, wherein keys from the first domain share only one ancestor with said keys from other domains (column 4: lines 40-60).

As per claim 8:

Sudia discloses a method, wherein varying levels of service are available and a group of users of a low-service level are allocated placebo keys providing no security, thereby to obviate a need to reconfigure other user's keys upon their invalidation (0090; 0138; 0139).

As per claim 9:

Sudia discloses a method, wherein the service is a dynamic service and its value is ephemeral and based upon its contemporaneous nature (0138; 0139).

As per claim 13:

Lotspiech discloses a computing entity adapted to manage distribution of security keys keys generated from an ancestral hierarchy and used to provide selective access to provision of a service, wherein invalidation of a key necessitates reconfiguration of each other key within the hierarchy to the extent another key and an invalidated key share common ancestry, the entity being adapted to:

define at least two groups of users of the service to whom keys have been issued (column 3: lines 5-21; column 4: lines 37-60; column 6: lines 20-37); issue keys to users from domains within the hierarchy upon the basis of their grouping (column 3: lines 11-20, lines 53-64; figure 4:36, 38; Column 7: lines 55-65).

Lotspiech does not explicitly disclose allocate within the hierarchy a distinct domain for each group of users. Sudia, in analogous art, however, teaches allocate within the hierarchy a distinct domain for each group of users (0046-0050). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Lotspiech to include allocate within the hierarchy a distinct domain for each group of users. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a system for securely using digital signatures in a commercial cryptographic system that allows industry-wide security policy and authorization information to be encoded into the signatures and certificates by employing attribute certificates to enforce policy and authorization requirements as suggested by Sudia in (0024).

12. Claims 10-12 and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia et al. (hereinafter referred to as Sudia, US Pub No.: 2002/0029337) in view of Lotspiech et al. (hereinafter referred to as Lotspiech, US Pat. No.: 7,039,803).

As per claim 10:

Sudia discloses a method of managing security key distribution to a plurality of users of a service comprising the steps of: defining levels of service provision (0014; 015; 0075); and allocating keys to users which are indicative to a service provider of the level of service to which they are entitled (Column 4: lines 37-50; column 10: lines 3-22).

Sudia does not explicitly disclose for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services. Lotspiech, in analogous art, however, teaches for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services (column 7: lines 15-25: short-lived key). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Sudia to include for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a grouping of users into (possibly overlapping) subsets of users, each subset having a unique, preferably long-lived subset key, and assigning each user respective private information as suggested by Sudia in (column 3: lines 10-20).

As per claim 11:

Sudia discloses a method, wherein the placebo keys operate in such a manner that a user is not able to perceive a difference between a functioning security key and a placebo key (Column 4: lines 36-52: short and long lived key).

As per claim 12:

Sudia discloses a method, wherein the service is dynamic and its value is ephemeral and based upon its contemporaneous nature (Column 4: lines 36-52: short and long lived key).

As per claim 14;

Sudia discloses a method of computing entity adapted to manage security key distribution to a plurality of users of a service by: defining levels of service provision (0014; 015; 0075); allocating keys to users which are indicative to a service provider of the level of service to which they are entitled (Column 4: lines 37-50; column 10: lines 3-22).

Sudia does not explicitly disclose for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services. Lotspiech, in analogous art, however, teaches for at least one level of service provision allocating placebo keys which do not provide security for the provision of the services (column 7: lines 15-25: short-lived key). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Sudia to include for

at least one level of service provision allocating placebo keys which do not provide security for the provision of the services. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to provide a grouping of users into (possibly overlapping) subsets of users, each subset having a unique, preferably long-lived subset key, and assigning each user respective private information as suggested by Sudia in (column 3: lines 10-20).

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art.

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T. G

Techane Gergiso

Patent Examiner

Art Unit 2137

August 26, 2007

Matthew Smithers

Matthew Smithers
Primary Examiner
Art Unit 2137